Jamcracker Disaster Recovery Plan

Chapter I - Introduction

PURPOSE

This manual is the Disaster Recovery Plan for facilities, systems, and personnel located at 19000 Homestead Road, Cupertino, California. Designs and produces computer software used in the production Jamcracker and Application service provider industries in addition to designing Jamcracker future releases. This manual establishes a structure to facilitate decision-making and provide a coordinated response to a disaster that may result in a disruption of production operations and processing.

SCOPE

The scope of this plan is restricted to the Disaster Recovery Planning for facilities and personnel used to keep Jamcracker production applications operational.

OBJECTIVES

The key objectives of this plan are:

To provide for the safety of employees and customers data first and foremost.

To ensure the continued survival of in the event of a disaster by protecting its personnel, systems, functions, and computer processing.

To reduce areas of risk which could affect end-user customer experience and revenue streams.

ASSUMPTIONS

The following assumptions were made in developing this plan:

- Life safety is the first priority.
- The disaster will occur at the worst possible time.
- There will not be an occurrence of two disasters concurrently (for example, two independent complexes in any given location affected at the same time).

- The disaster will be "complex specific" (for example, earthquake, bldg fire, bombing) disaster. The complex will be destroyed or unusable for an indeterminate period of time (weeks, not days).

- The municipal infrastructure will be fully operational and available in a disaster.

- Trained personnel will survive the disaster in order to implement recovery plans.

- Alternate Work Site facilities and off-site storage areas will survive the disaster.

- Dependent end-users are prepared to work in a degraded mode at backup sites for an indeterminate period of time. This may include using a reduced staff, working off-hours, postponing low priority tasks, etc.

LEVELS OF DISASTER

A disaster is defined as any event that creates an inability on part to provide production LAN/WAN systems and processing for an undetermined period of time. There are three levels of disasters. In order of increasing severity, they are:

- **MINOR -** This event has a minimum effect on overall operations and may go unnoticed by unaffected departments. Notification of this type of disaster may require some of operations to be suspended or critical personnel relocated for a short time. Examples: small fire, bomb threat, water damage, short-term power outage. This outage is determined to be about **ONE DAY** (i.e., in excess of one shift, but not longer than 24 hours.)

- **MAJOR -** This event has a greater effect on overall operations and may halt some operations temporarily. This type of notification may result in the relocation of some critical business operations to designated backup work sites.
  Examples: large fire, chemical spill, civil disturbance, wide area power outage. This outage is determined to be about **TWO DAYS** (i.e., 48 hours).

- **CATASTROPHIC** - This event has a devastating effect on all areas of operations, requires extensive outside assistance, and may disrupt normal operations for an extended period. Notification of this type of situation will require impacted operations to be relocated to designated backup work site(s). Examples:
  major fire, major chemical spill, major flooding, bombing. This outage is determined to be in excess of **THREE DAYS** (i.e., greater than 72 hours).

The disaster recovery plan is designed to facilitate recovery from a **CATASTROPHIC** disaster. This design ensures the plan can easily facilitate and direct the recovery process in the event of a lesser (e.g. Minor or Major) disaster.

EVENT DETECTION

The initial triggering of the disaster recovery plan is dependent upon established Event Detection procedures. Event Detection consists of General Emergency (Fire, Bomb Threat, Chemical Spill, etc.) and Problem Escalation (Hardware, Software, etc.) procedures. General Emergency procedures are maintained by Security who educates and trains employees in responding to an emergency of this nature. Event Detection procedures are maintained by System & Network Administration and utilized in day-to-day operations. As soon as an emergency exceeds established General Emergency or Problem Escalation guidelines, the Disaster Recovery plan will be activated.

NOTIFICATION & MOBILIZATION PLAN

As soon as a potential disaster has been detected, it is critical that the appropriate contacts are established and each given clear and concise information. The steps to notify and mobilize management, vendors, customers, and Disaster Recovery Team members are outlined as part of the Notification & Mobilization procedure. The procedure is divided into two (2) phases, Pre and Post Failure Assessment, clearly defining "who" needs to be notified prior to failure assessment and "who" needs to be notified once failure assessment has been completed and a disaster declared.

FAILURE ASSESSMENT

Following a disaster, an immediate failure assessment will be conducted to determine the extent of the impact on the primary facility and other required resources. A decision can then be made as to whether it will be necessary to implement the disaster recovery plan and migrate to the alternate work site. The failure assessment procedure includes roles and decision-making responsibilities and an investigation of items such as:

· Damage to the building and life support systems

· Disruption to voice and data communications links

. Disruption to production LAN/WAN systems and application environments

· Availability of vital records and other critical data

- Effect on staff
- Impact on other required resources

DECLARING A DISASTER

If Failure Assessment reveals the outage will exceed **THREE DAYS or 72 hours**, the disaster recovery plan will be implemented and relocation to the alternate work site to recover operations and processing initiated.

RECOVERY STRATEGY

The Disaster Recovery plan recovery strategy is designed to provide coordinated and comprehensive recovery operations. The recovery strategy consists of four (4) key components:

1. **Disaster Recovery Team -** Designated individuals organized to serve as the team that provides a coordinated response to an emergency. The team is under the direction of the Systems & Network Recovery Director who is accountable to the Vice President of Infrastructure.

2. **Disaster Recovery Plan** - A comprehensive plan, used by the Disaster Recovery Team, structured to facilitate decision-making and provide a coordinated response to an event that resulted in a disruption of LAN/WAN operations and processing.

3. **Off-Site Data Storage -** Frequent backup and storage of critical production data at an off-site storage vendor. The backup data can be easily retrieved, and delivered in a timely manner for system and application recovery.

4. **Alternate Work Site(s)** - A local alternate work site designated to recover the production LAN/WAN applications, systems, and processing following a catastrophic disaster. Refer to Appendix G-Alternate Work Site Implementation Procedure for detailed backup work site information.

Important Note: The above recovery strategy is not intended as the only course of action. Disaster Recovery personnel may need to modify the Plan or use other courses of action in order to fit specific circumstances.

RECOVERY TIMEFRAME

Within **TWENTY FOUR (24) HOURS** of initial notification of a potential disaster, the objectives of the Disaster Recovery Plan are to:

- Notify and mobilize Disaster Recovery Team personnel, management, vendors, customers, and the alternate work site.

- Assess and classify the severity of damage caused by the disaster.

- Declare a disaster and issue a recovery directive if a Catastrophic disaster occurred.

  Relocate operations and personnel to the alternate work site to restore department operations.

The timeframe to recover the LAN/WAN production systems and processing environment is outlined in Appendix J-LAN System & Application Priorities.

RECOVERY PHASES

Response to a disaster is divided into four (4) active phases plus a preliminary planning phase. The first active phase is triggered by the initial indication of an emergency.

Phase 0 **PLANNING**

This phase concentrates on planning for an initial response to an emergency.

Phase 1 **EVENT DETECTION**

This phase provides for the initial notification of designated individuals/civil authorities and evacuation of employees/customers once an emergency has occurred and is initially detected.

Phase 2 **NOTIFICATION & MOBILIZATION**

This phase provides for the notification and mobilization of Disaster Recovery Team and Management, for the assessment and classification of damage caused by the emergency, and for the declaration of a disaster and issuance of an appropriate Recovery Directive, if so required.

Phase 3 **ACTIVATE & MANAGE BUSINESS RECOVERY**

This phase provides for the activation of established and business unit recovery plans, for the relocation of operations to the alternate work site, for the restoration of affected business operations, and for the management of immediate and long-term recovery operations.

Phase 4 **RETURN TO PRIMARY FACILITY**

This phase provides for the return to the primary work facility. This phase is the responsibility of Facilities Management personnel. The disaster recovery plan does not address this phase of recovery.

MANAGEMENT & TEAM ROLES

The following management and team roles will be established when the plan is implemented:

- Recovery Team Manager
- Systems & Network Recovery Manager
- Systems & Network Recovery Team

Refer to Section III-Chapter IV Disaster Recovery Team Procedures for detailed information about the primary and alternate assignments and the key responsibilities for each position.

MANAGEMENT SUCCESSION PLAN

The disaster recovery plan has developed a succession plan in the event that key individuals are not available to fill assigned disaster recovery roles. Succession plans will be exercised if a primary candidate is unavailable for any reason (for example, injured, sick, on-vacation, etc.). Each Disaster Recovery team nominee has defined alternates capable of serving in his/her absence. In an absence, the first team alternate to be contacted immediately assumes the roles and responsibilities of the primary candidate.

UNIT FUNCTIONS & REQUIREMENTS

Detailed unit functions and requirements for are outlined in Appendix F-Unit Functions & Requirements.

LAN APPLICATION & SYSTEM PRIORITIES

LAN/WAN functions have been prioritized according to their importance to the continued operation of the business in the event of a disaster. Refer to Appendix J-LAN System & Application Priorities.

LAN POLICIES AND PROCEDURES IN A DISASTER

Established LAN policies and procedures will remain in effect during a disaster unless otherwise directed by management.

It may become necessary, during and after a disaster, for certain policies to be suspended in order to effect a timely response and recovery effort. Technical personnel will recommend and receive approval from management for the suspension of any policies/procedures.

Communications will be issued informing impacted users and Audit of the suspended polices/procedures and/or of any interim policies/procedures to be followed.

EMPLOYEE DISASTER HELP LINE

Security has an established phone line to provide up-to-date disaster information for employees. Help Line information will include building status, work schedules, system status, human resource news, etc. Refer to Appendix C-Key Internal Contacts for the Help Line phone number.

Chapter II – Notification & Mobilization

OVERVIEW

This section details the steps to be exercised by the Systems & Network Recovery Team Manager to notify and mobilize management, vendors, customers, and Disaster Recovery Team members once a potential disaster has been detected and initial notification of the occurrence of the emergency received.

STAFF NOTIFICATION CONSIDERATIONS

It is important that extreme care be exercised in notifying personnel of an emergency at a facility. This is especially important if the employees' family or friend answers the telephone and says the employee is not at home but working at the affected facility. Ask for the employee by name. If the employee is not home, **DO NOT INFORM** the family or friend that there is an emergency. Tell the person answering the phone to have the employee call you back at your current phone number. Provide each person contacted with the following information:

- A brief situation report.
- Your current location and phone number.
- The location of the alternate work site designated to recover production LAN systems and applications.
- Remind each team member contacted to bring their copy of the Disaster Recovery Plan.
- The phone number of the Employee Disaster Help Line to receive up-to-date disaster information.

If a team's primary named contact is unavailable and the alternate is selected, the alternate assumes full responsibility for the position. Attempts to notify the team's primary contact may be continued, as appropriate. If notification to a team's primary or alternate contact cannot be completed, appropriate management personnel must be notified.

NOTIFYING STAFF DURING & AFTER BUSINESS HOURS

To notify staff members of an emergency, first attempt to reach the employee via his/her pager. If contact is not made, the second attempt should be made to the employees' home phone number. If the employee still cannot be reached, the third attempt should be made to the employees' designated emergency contact.

PROCEDURE

The Notification & Mobilization procedure details specific steps to notify and mobilize designated management, vendors, internal units, customers, and members of the Disaster Recovery Team once notification of the occurrence of a potential disaster has been received. The procedure is divided into two (2) phases, PRE and POST FAILURE ASSESSMENT, to allow an orderly process from initial event notification to disaster declaration, with minimal disruption to employees.

PRE-FAILURE ASSESSMENT

1. LOG SITUATION REPORT

Log brief situation report from the initial notification of the emergency noting the nature and magnitude of the emergency, who has been notified (for example, fire, police), and the extent of damage, if available.

2. ALERT DEPARTMENT MANAGER

Contact management and brief he/she on the emergency. Collectively determine if activation of the Disaster Recovery Plan is warranted based on the nature of the emergency. If activation is warranted, continue with Step 3, else stop. Refer to Appendix A-Employee Phone List.

3. ALERT DISASTER RECOVERY TEAM

Contact and brief team members. Provide each member contacted with:

a. a brief situation report.
b. your current location and phone number.
c. a reminder to bring their copy of the Disaster Recovery Plan.

Request team members to mobilize and arrive at the affected facility to participate in recovery operations. Refer to Appendix A-Employee Phone List.

4. ALERT MANAGEMENT

Notify and brief members of management (e.g. Marketing, Public Relations, etc.). The System & Network Recovery Team manager is responsible for this task unless otherwise delegated. Refer to Appendix C-Key Internal Contacts.

5. ALERT THE ALTERNATE WORK SITE

Contact and alert the alternate work site. Request alternate work site contacts to be prepared to support recovery operations and processing. Refer to Appendix F LAN Alternate Work Site Implementation Procedure.

6. ALERT OFF-SITE DATA STORAGE VENDOR

Contact and alert the off-site data storage vendor. Request vendor to be prepared to retrieve and deliver backup data if a disaster is declared. Refer to Appendix B-Vendor Phone List.

7. ALERT KEY HARDWARE & SOFTWARE VENDORS

Contact and alert hardware and software vendors based on the severity and nature of the emergency. Request vendors to be prepared to support recovery operations if a disaster is declared. Refer to Appendix B-Vendor Phone List.

8. ALERT KEY INTERNAL CONTACTS

Contact and alert key internal units and their contacts. Refer to Appendix C-Key Internal Contacts Phone List.

9. EXECUTE & COMPLETE FAILURE ASSESSMENT

With the aid of Security, Facility, and Disaster Recovery Team members, perform and complete the Failure Assessment process. Refer to the Chapter III-Failure Assessment procedure starting on Page 3-5 of this chapter.

10. IF A CATASTROPHIC DISASTER HAS OCCURRED

If Failure Assessment reveals a Catastrophic Disaster has occurred, execute Post-Failure Assessment tasks that begin on Page 3-4 of this chapter. If Failure Assessment reveals that a lesser level of disaster has occurred (Minor or Major) and operations can continue at the affected facility, re-notify personnel and de-escalate the emergency status mobilizing only those needed to restore operations.

POST-FAILURE ASSESSMENT

If Failure Assessment reveals that a CATASTROPHIC disaster has occurred at the facility, the following steps must be exercised:

1. DECLARE A DISASTER & ISSUE RECOVERY DIRECTIVE

Formally declare a disaster and issue an appropriate Recovery Directive.
Refer to Chapter III-Declaring a Disaster on Page 3-13 of this chapter.

2. DISTRIBUTE THE RECOVERY DIRECTIVE

Distribute the Recovery Directive corporate wide. Distribution must occur via all available hardcopy, voice, and electronic mediums.

3. ACTIVATE & RELOCATE TO THE ALTERNATE WORK SITE

Re-notify alternate work site contacts and declare a disaster. Request the alternate work site to be prepared immediately for recovery operations. Refer to Appendix F-Alternate Work Site Implementation Procedure.

4. RETRIEVE PRODUCTION DATA FROM OFF-SITE STORAGE VENDOR

Re-notify off-site data storage vendor and retrieve production backup media. Refer to Appendix J-Data Backup & Off-Site Storage for steps to retrieve data.

5. RE-NOTIFY MANAGEMENT, INTERNAL UNITS, VENDORS, & CUSTOMERS

Re-notify and mobilize, as required, the following individuals of the disaster declaration and recovery directive:

- Management
- Vendors
- Key Internal Contacts

Customers

6. MANAGE IMMEDIATE & LONG-TERM RECOVERY OPERATIONS

Manage immediate and long-term recovery operations from the alternate work site until processing can be returned to the primary facility.

FAILURE ASSESSMENT

OVERVIEW

This section details the steps to be used to inventory damage to facility resources. Security and Facilities Management personnel will initially determine, with the aid of local authorities, if and when access to the facility will be granted. As soon as Failure Assessment can be safely performed, the System & Network Recovery team will evaluate:

1. Status of Personnel (injured, etc.).
2. Damage to the Physical Plant / Co-location (structural integrity, utilities, etc.).
3. Damage to Production Networks & Systems (servers, routers, etc.).
4. Damage to Operational Resources (office equipment, phones, etc.).

Once these key components have been evaluated, the System & Network Recovery team will:

1. Summarize the damage by classifying the level of the disaster (Minor, Major, or Catastrophic) and the estimated outage period (hours, days, months).
2. Communicate the Failure Assessment results to the Department Manager for final review and concurrence.

If a Catastrophic level disaster has occurred, the Systems & Network Recovery Team Manager will formally declare a disaster and issue an appropriate recovery directive to restore production LAN/WAN operations. If a lesser category of disaster has occurred (Minor or Major), selected components of the disaster recovery plan will be used, as required, to recover and restore operations.

IMPORTANT CONSIDERATION

It is critical to recognize that access could be denied to the facility for several days before entry is granted to perform Failure Assessment. Failure Assessment may need to be performed physically away from the facility using **ONLY** the information provided by emergency service personnel. The System & Network Recovery team must be prepared to quickly evaluate the event and determine if a disaster must be declared without support of the Failure Assessment process.

PROCEDURE

The System & Network Recovery team in coordination with Security and Facility Management personnel will assess damage to the facility in the order described below. Failure Assessment work sheets to inventory damage may be found starting on Page 3-7 of this chapter. The steps to perform Failure Assessment are:

1. LIST DAMAGE TO THE PHYSICAL PLANT

List the obvious damage to buildings, utilities, air conditioning, telephone service, security systems, and work space, etc.

2. LIST DAMAGE TO PRODUCTION NETWORKS & SYSTEMS

Servers
Tape Drives
Disk Drives
Routers
Hub Configurations
Communications (Voice & Data)
Critical Data on Disk Drives & Backup Media

3. LIST DAMAGE TO OPERATIONAL RESOURCES

Summarize damage to office equipment, files, end-user work stations, phones, etc. on affected floor(s). Damage may be sustained in any or all of several categories. Quickly look at the elements of each category, first to determine whether or not there has been any damage within the category, then if damage has been sustained.

4. SUMMARIZE EFFECTS OF THE DAMAGE

Summarize damage to the affected facility. Define the severity level of the disaster (minor, major, catastrophic) and the estimated outage period (hours, days, months).

5. COMMUNICATE FAILURE ASSESSMENT RESULTS

Communicate completed Failure Assessment to the Department Manager for final review and concurrence.

FAILURE ASSESSMENT WORKSHEET
Page 1 of 6

PHYSICAL PLANT DAMAGE

Date: ___ / _____ / ____

Time: ___ : _____ AM / PM

Facility Affected: ____

Floors Affected: ____

Structural Integrity / Work Space

____

____

Jamcracker Operations

FAILURE ASSESSMENT WORKSHEET
Page 2 of 6

PHYSICAL PLANT DAMAGE

Utilities (Water, Sewer, Electricity)

____

Entry / Exit / Parking

____

____

____

____

____

____

____

____

____

____

Telephone Service

____

____

____

____

____

Jamcracker Operations

FAILURE ASSESSMENT WORKSHEET
Page 3 of 6

PRODUCTION NETWORK & SYSTEMS

Floor: _______

Servers, Disk Drives, Tape Drives

____

____

____

____
____
____
____
____
____
____
____
____
____
____
____
____
____

Routers & Hub Configurations

____
____
____
____
____
____
____

Jamcracker Operations

FAILURE ASSESSMENT WORKSHEET
Page 4 of 6

PRODUCTION NETWORK & SYSTEMS

Floor: _______

Data Communications

Critical On-Site Production Data

Jamcracker Operations

FAILURE ASSESSMENT WORKSHEET
Page 5 of 6

OPERATIONAL RESOURCE DAMAGE

Floor: _______

Office Equipment, PC's, Phones, Terminals, etc.

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Note: Use a new sheet for each floor affected.

Jamcracker Operations

FAILURE ASSESSMENT WORKSHEET
Page 6 of 6

FAILURE ASSESSMENT SUMMARY

Level of Disaster: **Minor / Major / Catastrophic**

Projected Outage : **_____ Hours/Days/Months**

Final Comments:

____

____

____

____

____

____

____

____

____

APPROVE / CONCUR

The following individuals approve and concur with FAILURE ASSESSMENT.

Approve
Systems & Network Recovery Team Manager

- - - - - - - - - - - - - - - -
Signature/Date

Concur
Department Manager

- - - - - - - - - - - - - - - -
Signature/Date

Declaring a Disaster

OVERVIEW

The Systems & Network Recovery Team Manager is authorized to declare a disaster and activate the disaster recovery plan to restore production networks and systems. If the Systems & Network Recovery Team Manager is not available, his/her alternate is authorized to declare a disaster. If the alternate is not available, any two (2) concurring System & Network Recovery Team members can approve the Failure Assessment and declare a disaster. This section outlines the steps to declare a disaster and issue a recovery directive to the affected units.

PROCEDURE

The Systems & Network Recovery Team Manager will exercise the following steps to declare a disaster and issue a formal recovery directive once Failure Assessment has been completed by the System & Network Recovery Team:

1. GATHER FAILURE ASSESSMENT RESULTS

Gather verbal or written damage assessment from the System & Network Recovery Team. The assessment summarizes facility and technology resource damage in addition to defining the severity level of the disaster (minor, major, catastrophic) and the projected outage period (hours, days, months).

2. REVIEW FAILURE ASSESSMENT RESULTS

Review the Failure Assessment report. If the Systems & Network Recovery Team Manager agrees a CATASTROPHIC disaster has occurred and the disaster recovery plan must be activated, proceed with formal disaster declaration by completing and issuing the recovery directive described in Step 3.

3. DECLARE DISASTER & COMPLETE RECOVERY DIRECTIVE

Complete the Recovery Directive on Page 3-15 of this chapter. The Recovery Directive defines, in brief terms, what has occurred, what has been damaged, the level of disaster, and lastly, recovery strategy to restore business operations.

4. DISTRIBUTE RECOVERY DIRECTIVE

Distribute the Recovery Directive corporate wide via hardcopy, electronic mail, and voice mediums to the units impacted by the loss of operations.

5. PROCEED WITH POST-FAILURE ASSESSMENT TASKS

Return to Post-Failure Assessment Tasks outlined on Page 3-4 of this chapter and execute all remaining tasks.

RECOVERY DIRECTIVE

EMERGENCY SPECIFICS (Who, what, when, where)

Date: ___ / _____ / ____

Time: ___ : _____ AM / PM

Facility: ____

Emergency Summary:

____

____

____

____

____

____

____

____

____

____

DAMAGE ASSESSMENT SUMMARY

Level of Disaster: Minor / Major / Catastrophic

Projected Outage : _____ Hours/Days/Months

Damage Assessment Summary:

____

____

____

Jamcracker Operations

RECOVERY DIRECTIVE

RECOVERY STRATEGY

Based on the severity level and estimated outage period, the Systems & Network Recovery Team Manager in coordination with the System & Network Recovery Team issues the following directive to recover from the disaster:

Recovery Strategy:

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

APPROVE

The following approves with the stated Recovery Directive.

Approve
Systems & Network Recovery Team Manager

- - - - - - - - - - - - - - - -
Signature/Date

CHAPTER III- System and Network Recovery Team

OVERVIEW

This chapter outlines the general responsibilities of the Systems & Network Recovery Team in responding to a disaster. Disaster Recovery team members may need to modify the Plan or use other courses of action in order to fit specific circumstances.

The Systems & Network Recovery Team, in an emergency, operates under the direction of the Manager and consists of the following:

The Systems & Network Recovery Team Manager manages the Systems & Network Recovery Team and is accountable to the Department Manager. Individual team members are nominated by the team leader. Team leaders are responsible for ensuring that all required positions within his/her team are filled and properly trained at all times.

Recovery Manager

The Recovery Manager is responsible for the following tasks in the event of a disaster

- Receive initial notification of the potential disaster from the Systems & Network Recovery Team Manager or designated Disaster Recovery Team member. Assess the potential disaster situation.

- If the emergency warrants it, authorize the activation of the Disaster Recovery Plan.

- Travel to the facility to assess damage to systems and resources.

- Notify management and brief on the potential disaster event.

- Make high level safety and system recovery decisions throughout the term of the disaster.

- Participate in and review Failure Assessment findings with the Systems & Network Recovery Team.

- If Failure Assessment reveals a catastrophic disaster has occurred, declare a disaster and issue an appropriate recovery directive to restore operations.

- Relocate to the alternate work site to begin recovery operations.

- Establish Emergency Command Center at alternate work site to coordinate recovery resources, personnel, and facilities.
- Hold daily status meetings with members of the Disaster Recovery Team and Management for duration of the recovery effort.
- Manage the immediate and long-term recovery activities of the System & Network Recovery team.
- Direct the emergency workflow of critical functions, applications, and resources.
- Establish funds for the immediate needs of the disaster recovery effort.
- Authorize and account for expenditures related to the disaster recovery effort.
- Report progress and make recommendations to Management.

System and Network Recovery Manager

The Systems & Network Recovery Team Manager is responsible for the following tasks in the event of a disaster

- Receive initial notification of the emergency. Notification of the event may come via established General Emergency (Fire, Bomb Threat) or Problem Escalation (Software, Hardware, etc.) procedures.
- Log brief situation report from the initial notification of the emergency noting the nature and magnitude of the emergency, who has been notified (for example, fire, police), and the extent of damage, if available.
- Notify the Manager or designated alternate and brief he/she on the emergency.
- Request authorization from the Department Manager to activate the disaster recovery plan based on the severity of the emergency.
- Notify and mobilize Disaster Recovery Team members. Request team members to assemble at the damaged facility.
- Notify and alert alternate work site personnel.

- Notify and alert management.

- Notify and alert vendors and internal contacts.

- Perform Failure Assessment with support of Security and Building Facility personnel identifying damage to the Physical Plant, Production Systems & Networks, and Operational Resources.

- Summarize damage to the affected facility. Define the severity level of the disaster (minor, major, catastrophic) and the estimated outage period (hours, days, months).

- If a CATASTROPHIC disaster has occurred, formally declare a disaster and issue a recovery directive with the authorization of the Manager or designated alternate.

- Activate the alternate work site to commence recovery of critical functions and processing.

- Activate vendors, internal contacts, and customers based on the severity level and estimated outage period.

- Mobilize and relocate Disaster Recovery team members to the alternate work site to launch system and network recovery operations.

- Establish Emergency Command Center at alternate work site to coordinate and direct resources.

- Manage the immediate and long-term responsibilities of the Disaster Recovery team.

- Direct the restoration of critical end-user applications and environments following pre-established priorities.

- Make recommendations and report recovery progress to management on a daily basis.

The Systems & Network Recovery Team

Systems & Network Recovery Team is responsible for the following tasks in the event of a disaster

- Receive initial notification of the disaster from the Systems & Network Recovery Team Manager or his/her designated alternate.

- Assemble at the damaged facility or other location as designated by the Systems & Network Recovery Team Manager.
- Assist in notifying and alerting alternate work site personnel, vendors, internal contacts, and customers as directed by the Systems & Network Recovery Team Manager.
- Assist in identifying damage to Production Systems & Networks and Operational Resources.
- Assist in defining the severity level of the disaster (minor, major, catastrophic) and the estimated outage period (hours, days, months).
- If a catastrophic disaster has occurred and a disaster declared, support activation of the alternate work site to commence recovery of critical functions and processing.
- Activate required management, vendors, internal contacts, and customers to recover systems and processing.
- Relocate to the alternate work site to begin system and network recovery operations.
- Restore critical end-user applications and environments following pre-established priorities and recovery procedures.
- Make recommendations and report recovery progress to the Systems & Network Recovery Team Manager on a daily basis.

Chapter IV – Staff and Logistical Support

OVERVIEW

This section outlines general personnel assembly, staffing, notification, and logistical support procedures in the event of a disaster.

PERSONNEL ASSEMBLY

The following general Personnel Assembly instructions will be followed for events occurring **"During"** and **"After Business Hours"**.

During Business Hours: If an emergency occurs during business hours, employees will evacuate and assemble at pre-defined locations away from the affected facility. The Systems & Network Recovery Manager or designated alternate will assemble personnel, assess the emergency, and activate the disaster recovery plan, if required.

After Business Hours: If an emergency occurs after business hours, employees will be contacted by the Systems & Network Recovery Manager or designated alternate. Employees will be briefed on the emergency and asked to report to the facility or designated alternate work site.

Important Note: Employees receiving notification of the disaster from outside media sources (radio, television) are directed to contact the Employee Disaster Help Line and Systems & Network Recovery Team Manager for information and instructions.

STAFF NOTIFICATION STRATEGY

To notify staff members in an emergency, first attempt to notify the employee via his/her alphanumeric pager. If contact is not made, the second attempt should be made to the employees' home phone number. If the employee still cannot be reached, the third attempt should be made to the employees' designated emergency contact.

STAFFING

It is assumed that general staff will be able to fill their normal roles. If it is necessary to locate alternates, management will look first to internal technical personnel to provide the skills needed. If internal personnel cannot meet technical needs, management will look to external sources (vendors, consultants, etc).

STAFF WORK SCHEDULES

End-user work schedules and locations will be coordinated with alternate work site and management.

LOGISTICAL SUPPORT FUNCTIONS

Staff Transportation Plan: It is assumed that staff will use personal transportation to relocate to the alternate work site for the duration of the disaster. Car and van pooling will be used as needed based on employee needs.

Production Backup Media Transportation Plan: The off-site storage vendor (ARCUS Data Security) will transport production backup media to the designated alternate work site upon authorization from designated personnel.

Interoffice/External Mail: Personnel will contact internal mail personnel and advise them of the new work site address and unit number.

RESTORATION OF OPERATIONS TO PRIMARY WORK SITE

There is no pre-defined plan to restore the original facility. This will be the responsibility of Facilities Management.

CHAPTER V – APPENDICES

Employee Phone List

Vendor Phone List

Key Internal Contact Phone List

Customer Phone List

Disaster Recovery Plan Checklist

Unit Function and Requirements

UNIT FUNCTION

Systems & Network Administration provides technical support, application development, network connectivity, and maintenance to production LAN/WAN systems and applications.

UNIT STAFFING STRATEGY

All System & Network Recovery team members will relocate to the alternate work site and establish operations. End-user staffing will depend on the available alternate work site space. Critical end-users will be asked to relocate to the alternate work site while non-critical users will be asked to use home based personal computers to access the alternate work site system and applications.

UNIT ORGANIZATIONAL STRUCTURE

The organizational structure, in the event of a disaster, will remain consistent with the current day-to-day organizational structure. A current organizational chart is attached on Page F-3 of this chapter.

SERVER & END-USER COMPUTER REQUIREMENTS

Server and end-user computer requirements are detailed in Appendix H-Server & End-User Configuration.

DATA & VOICE CONNECTIVITY REQUIREMENTS

Data and voice connectivity requirements are detailed in Appendix I-Network Configuration.

END-USER WORKSTATION REQUIREMENTS

A minimum of 35 end-user workstations per shift with dedicated computer access to the restored systems and applications are required at the alternate work site.

END-USER TELEPHONE REQUIREMENTS

A minimum of 35 telephones per shift need to be made available at the alternate work site.

OFFICE SUPPLY REQUIREMENTS

A minimum of three (3) day's worth of business supplies need to be on-site to support the staff.

SPECIAL FORMS REQUIREMENTS

There are no special form or supply requirements.

SPECIAL EQUIPMENT NEEDS

There are no special needs at this time.

Alternate Worksite Selection

PURPOSE

The purpose of the Alternate Work Site Implementation procedure is to detail the specific steps to activate backup facility personnel and resources needed to support disaster recovery operations following a catastrophic disaster.

ALTERNATE WORK SITE

The ALTERNATE WORK SITE selected to backup System & Network operations is the **Jamcracker Service Center** department located at:

Jamcracker
4940 South Wendler Drive
Suite 201
Tempe, Arizona 85282

A detailed alternate work site facility map and floor plan is provided as the last two pages of this chapter.

ALTERNATE WORK SITE CONTACTS

In the event of a catastrophic disaster, contact ONE of the following individuals to activate the backup work site:

ALTERNATE WORK SITE CONTACTS PHONE LIST

PRIMARY & ALT CONTACT	WORK	ALTERNATE PHONE NUMBERS	HOME	COMMENT
P - 24 Hour Pager A - A - A - A -				

ACTIVATING THE ALTERNATE WORK SITE

1. Contact **ONE** of the Alternate Work Site contacts listed in the Alternate Work Site Contacts Phone List on Page G-1. Provide the alternate work site contact with a brief situation report; advise him/her of the disaster and the need to begin recovery of the system and applications.

2. Relocate Disaster Recovery Team members to the alternate work site facility. Refer to detailed facility map and floor plan attached as the last two pages of this chapter.

3. Meet the alternate work site contact at the backup facility.

4. Secure physical and system access for Disaster Recovery Team Members. This includes physical access to the main facility, access to the alternate work site areas, and system access to the backup systems used to recover operations.

5. Begin restoration of system and application environments using information provided in the disaster recovery plan.

Server & End-User Configuration

Network Configuration

System and Application Priorities

OVERVIEW

Each end-user application has been prioritized based on its importance to the continued operation of the business and will be restored based on its criticality. Applications will be restored in order of most to least critical.

BUSINESS IMPACT ANALYSIS

In order to prioritize end-user applications, a Business Impact Analysis (BIA) was completed for each application to measure the quantitative and qualitative effects expected if the function could not be performed over cumulative periods of 1, 2, 3, 10, and 30 days. Applications were then prioritized from most to least critical based on each
applications total level of quantitative and qualitative effect. The application with the greatest quantitative and qualitative impact was deemed most critical, second greatest quantitative and qualitative impact was deemed second most critical, etc. The completed BIA is attached starting on Page J-2 of this chapter.

SYSTEM & APPLICATION PRIORITIES

The priority of applications, based on the results of the BIA and technical personnel input, are as follows:

Critical Applications - Restored Within 12 hours
1. Jamcracker Production Operations
2. E-Mail

3. Backup Systems

Non-Critical Applications - Restored Within 48 hours

1. 3rd Party Tools
2. Development Tools

All applications will be restored within 72 hours of the disaster. The applications will be queued for restoration at the alternate work site in the above order. Application restoration priorities could be changed based on the conditions and requirements of the actual event.

LAN Backup and Offsite Retrieval

OVERVIEW

Data backup and off-site storage procedures are necessary to ensure that production data is available for processing in the event the primary on-site data is destroyed and or corrupted. Data is stored off-site for all systems in the LAN/WAN environment.

OFF-SITE STORAGE VENDOR

ARCUS (Iron Mountain) Data Security, Inc. has been contracted to pick up production backup media and relocate it to off-site storage on a weekly basis.

BACKUP RESPONSIBILITY

The Systems & Network Administration Director is directly responsible for managing data backup and off-site storage procedures.

BACKUP SCHEDULE & RETENTION

Backups are run nightly, Seven (7) days a week. Each night, full backups are completed on all production system.

ARCUS Data Security picks up production backup media once a week on **Monday's** and retains the media off-site for six (6) weeks. All backup tapes are recycled after a 6 week retention period. A Yearly Snap shot is also stored off-site

PRODUCTION DATA EXPOSURE

There is one (1) week worth of backup media on-site at all times. The maximum amount of data that could be potentially lost in event of a disaster is 1 full week. A full dump encompasses approximately 500 GB of data on a weekly basis.

SERVER BACKUP METHODOLOGY

Data residing on the Sun File Server environment are backed up using Veritas NetBackup software. Data residing on other machines, including the SPARC Storage Arrays, are also backed up using Veritas NetBackup. Retrieval of data from the backup media, for all environments, is accomplished using the data retrieval functions of the appropriate backup software packages.

RETRIEVING OFF-SITE DATA IN A DISASTER

The steps to retrieve production backup media in an emergency are as follows:

1. CONTACT ARCUS DATA SECURITY

Contact ARCUS Data Security at XXX-XXX-XXXX or XXX-XXX-XXXX, 24 hours a day, 7 days a week. You must be pre-authorized to contact ARCUS and request retrieval and delivery of data. Refer to Authorized Caller List on Page K-3 of this chapter.

2. PROVIDE ARCUS WITH KEY ACCOUNT INFORMATION

a. Account Number is <XXX>
b. Your Name and Current Phone Number
c. ARCUS Authorization Code (Must be a 1 or 2)
d. Announce a disaster has been declared and production media must be delivered to the location designated to recover operations.

ARCUS personnel will verify your information and authorize the request.

3. RELOCATE DATA TO ALTERNATE WORK SITE

Request ARCUS to deliver production backup media to the designated alternate work site. Refer to Appendix G-Alternate Work Site Implementation procedure for alternate work site address information.

AUTHORIZED CALLER LIST

ARCUS Data Security requires a caller to be on the "Authorized Caller" list before data will be retrieved and delivered to a designated alternate work site. The current authorized caller list to retrieve production data is:

	ARCUS	

Employee Name	Authorization Code	Authorization Level
	1	Can retrieve data in a disaster
	1	Can retrieve data in a disaster
	2	Can retrieve data in a disaster
	2	Can retrieve data in a disaster
On-Duty Guard	3	Sign for pickup/delivery only

System and Application Recovery

OVERVIEW

The System & Application Recovery procedure details the steps to restore the systems, applications, network communications, and end-user environments at the alternate work site.

ENVIRONMENT RESTORATION TIMEFRAME

The timeframe to restore critical applications and network environments, based on current configuration and volumes, is **Three (3) hours.** The timeframe to restore non-critical applications is **Twelve (12) hours.**

APPLICATION RESTORATION PRIORITIES

Each end-user application has been prioritized based on its importance to the continued operation of the business and will be restored based on its criticality. Applications will be restored in order of most to least critical. Refer to Appendix J-System & Application Priorities.

PRIMARY DATA USED IN RESTORATION

It is assumed that **ALL** on-site data has been destroyed and the primary data to be used in restoration will be the data stored off-site. The production data stored off-site is 1 week old with respect to the current production day. Refer to Appendix K-Data Backup & Off-Site Storage.

RESTORATION RESPONSIBILITY

The Systems & Network Recovery Team is directly responsible for managing the recovery of the system, application, and network environments.

END-USER SYSTEM VALIDATION

Designated end-users will be involved throughout the restoration process to verify the reconstructed application and network environments.

SYSTEM RESTORATION PROCEDURE

The high-level steps to restore the system, application, and network environments are as follows:

1. Establish physical and system access for Disaster Recovery team members at the alternate work site and its associated computer systems. Twenty-four hour access must be secured to enter the building, computer related work areas, and LAN/WAN systems required to restore the environment.

2. Retrieve backup supplies stored at the alternate work site. Supplies include day-to-day work supplies in addition to copies of the disaster recovery plan.

3. Acquire DLT tape drive(s) to support recovery at the alternate work site. If the alternate work site does not currently support or use 8mm tape drive(s). The tape drive may need to be purchased from an available computer supply store.

4. Retrieve production backup tapes from the ARCUS off-site storage facility.
   Deliver production to location designated to recovery systems and applications. Refer to Appendix K-Data Backup & Off-Site Storage for retrieval procedures.

5. Make appropriate changes for mounting of alternate work site file systems to restore data from the off-site backup media.

6. Restore systems, applications, and data in order of criticality. Refer to Appendix J-System and Application Priorities for a prioritized listing.

7. Develop a system restoration and staff work schedule based on current work schedules. The schedule must include a timeframe for the restoration of data, a timeframe for critical personnel to work second shift, and a timeframe for non-essential staff to work.

8. Provide periodic daily updates to management and end-users, advising them of scheduled system and application restoration and expected completion time.

9. Contact Tier II Network support and request ACL changes to reflect the network(s) software is being installed at the alternate work site.

10. Re-route DSL and remote access modem lines to the alternate work site. Contact MCI/WorldCom to execute the re-route procedure within 48 hours.
11. Request key end-users to be available to validate systems, applications, and connectivity, as each environment is restored and on-line.

12. Review the restored environment with key end-users identifying missing data, systems, connectivity, etc.

13. Contact equipment vendors to provide hardware/software not available at alternate work site. Inquire about loaner and rental equipment.

14. Contact purchasing contacts and inform them of upcoming equipment replacement orders.

15. Contact hardware vendors and request equipment replacement options. Delivery of equipment must occur on an overnight basis.

DR Plan Maintenance

PURPOSE

A Disaster Recovery Plan is only as valid as the information it contains. To ensure that the Plan can be used effectively in an emergency, it must be accurate, timely and complete. It is imperative, therefore, that the Plan be reviewed often and updated as necessary.

MAINTENANCE RESPONSIBILITY

The System & Network Recovery Team Manager is responsible for ensuring that the plan is maintained and revised as needed to reflect the current environment. In order to accomplish this, he/she must ensure that plan procedures and requirements are properly followed in addition to ensuring that reviews and revisions to the Plan are made as outlined in this section.

PLAN REVIEW

ANNUAL REVIEW --- Every year in January, the System & Network Recovery Team Manager will review the entire Disaster Recovery Plan with the individual disaster recovery team members of the System & Network Recovery Team.

ADDITIONAL REVIEWS --- In addition to the once-a-year comprehensive review of the Plan, additional reviews of certain segments of the plan will be conducted throughout the calendar year. The table on the following page details the entire Plan in segments, the review responsibility, and recommended review frequency.

REQUESTS FOR PLAN REVISIONS

Any employee requesting revisions to the Plan must submit a written request to the System & Network Recovery Team Manager for evaluation. If the request is approved, the System & Network Recovery Team Manager will revise the Plan appropriately.

PLAN SEGMENT REVIEW SCHEDULE

The review schedule for each segment of the Disaster Recovery Plan is as follows:

PLAN SEGMENT	REVIEW FREQ	REVIEW RESPONSIBILITY
Introduction	Annual	Sys & Net Recovery Team Mgr
Event Detection	Semi-Annual	Sys & Net Recovery Team Mgr
Notification & Mobilization	Semi-Annual	Sys & Net Recovery Team Mgr
Failure Assessment	Semi-Annual	Sys & Net Recovery Team Mgr
Declaring a Disaster	Semi-Annual	Sys & Net Recovery Team Mgr
DR Team Procedures	Semi-annual	Sys & Net Recovery Team Mgr
Staff & Logistical Support	Semi-Annual	Sys & Net Recovery Team Mgr
Appendices	Quarterly	Sys & Net Recovery Team Mgr Sys & Net Recovery Team

DISTRIBUTION OF REVISIONS

A cover memorandum giving instructions for inserting and removing documents from the manual is sent to each manual holder with each update. For each update, do the following:

- Read cover memo carefully.
- Remove obsolete or superseded documents if directed to do so.
- Place revisions in proper order in the manual.

- File the cover memo in the back pocket of the Plan so a living record of updates exist.

PURPOSE

The Disaster Recovery Plan manual is issued to the System & Network Recovery Team Manager, to Disaster Recovery Team members, and to selected members of management. Copies of this manual are additionally maintained at the alternate work site. Additional copies of this plan may be stored at other sites as considered appropriate by the Systems & Network Recovery Team Manager.

The Disaster Recovery Plan manual and / or its individual pages are not to be issued to individuals who are not employee's without the approval of the System & Network Recovery Team Manager.

It is the responsibility of employees to return Disaster Recovery Plan manuals to the System & Network Recovery Team Manager should their employment with cease. The System & Network Recovery Team manager maintains a current manual distribution list on the following page.

DISTRIBUTION TABLE

The following table outlines the current distribution list for the Disaster Recovery Plan:

TITLE	OFFICE COPY	HOME COPY	TOTAL
Technology Manager	**Yes**	**Yes**	**2**
Department Manager	**Yes**	**Yes**	**2**
Systems & Network Recovery Team Manager	**Yes**	**Yes**	**2**
Systems & Network Recovery Team Members	**Yes**	**Yes**	**6**
Alternate Work Site	**Yes**	**No**	**2**
Alternate Work Site Manager	**Yes**	**No**	**1**
ARCUS Data Security Off-site Storage	**Yes**	**No**	**1**
Totals			**16**

Training and Testing

PURPOSE

The System & Network Recovery Team Manager is responsible for managing testing and training activities related to the disaster recovery plan. The objective of testing and training is to provide employees with disaster prevention techniques in addition to the appropriate actions to take should a disaster occur.

TRAINING & TESTING RESPONSIBILITY

The System & Network Recovery Team Manager is responsible for testing and training activities related to disaster recovery planning.

TRAINING & TESTING PROGRAMS

The System & Network Recovery Team Manager manages the following training programs:

- **Annual Disaster Recovery Orientation Training** is mandatory for System & Network Recovery Team members and designated members of management.

- **Annual Disaster Recovery Testing** is mandatory for System & Network Recovery Team members and designated members of management.

TRAINING SCHEDULE

Annual Disaster Recovery Orientation Training - Sessions conducted on a semi-annual basis for each disaster recovery team member. The session agenda is:

1. Overview of Disaster Recovery Plan
2. Event Detection Procedures
3. Notification & Mobilization Procedures
4. Disaster Recovery Team Structure
5. Disaster Recovery Team Responsibilities
6. Disaster Recovery Team Procedures
7. Individual Team Member Responsibilities
8. Appendices Review

TESTING SCHEDULE

Annual Disaster Recovery Testing - The Systems & Network Recovery Team Manager will conduct an annual test exercise to test the accuracy and completeness of the Disaster Recovery Plan in addition to confirming the ability to recover processing and operations. A test of the Disaster Recovery plan will include:

1. Retrieving all recovery materials from off-site storage locations.
2. Relocating to the designated alternate work site.
3. Executing and validating the written disaster recovery plan:
    a. Notification & Mobilization Procedure
    b. Disaster Recovery Team Procedures
    c. Alternate Work Site Implementation Procedure
    d. Employee, Vendor, Customer, and Key Contact Phone Lists
    e. Off-Site Data Retrieval Procedure
    f. System & Application Recovery Procedure
4. Restoring critical applications and validating recovered environments.
5. Updating the Disaster Recovery plan to reflect testing results.

IMPORTANT NOTE: Current guidelines require one (1) annual test of the disaster recovery plan. It is recommended that exceed this guideline and implement a semi-annual testing schedule. Testing semi-annually provides personnel with additional experience and confidence in recovering the system and network environments in addition to further validating the written plan, backup data, and alternate work site.